

February 25, 2010

**VIA ELECTRONIC FILING**

Marlene H. Dortch, Secretary  
Office of the Secretary  
Federal Communications Commission  
445 12th Street, S.W.  
Suite TW-A325  
Washington, DC 20554

**Re: Annual 47 C.F.R. § 64.2009(e) CPNI Certification  
EB Docket No. 06-36  
FCC Filer ID: 826561 / FRN: 0016339814**

Dear Ms. Dortch:

Faircall Corporation, by its attorneys and pursuant to Section § 64.2009(e) of the Commission's rules, hereby submits its 2009 CPNI Certification and Accompanying Statement. If there are any questions regarding this submission, please contact the undersigned.

Respectfully submitted,



Michelle W. Cohen  
Counsel to Faircall Corporation

Enclosures

cc: Best Copy and Printing, Inc.  
(via e-mail [FCC@BCPIWEB.COM](mailto:FCC@BCPIWEB.COM))

BEFORE THE  
FEDERAL COMMUNICATIONS COMMISSION  
WASHINGTON, D.C. 20554

**EB Docket No. 06-36**

**ANNUAL 47 C.F.R § 64.2009(e) CPNI CERTIFICATION**

Annual 64.2009(e) CPNI Certification for 2009

Date filed: February 24, 2010

Name of company covered by this certification: **Faircall Corporation**

Form 499 Filer ID: **826561**

Name of signatory: **Gregorio Galicot**

Title of signatory: **President**

I, Gregorio Galicot, President of Faircall Corporation, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (*i.e.*, proceedings instituted or petitions filed by a company at either state commissions, the court system or at the Commission against data brokers) against data brokers in the past year.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47 C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. Faircall Corporation also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed

A handwritten signature in black ink, consisting of several loops and a long horizontal stroke, positioned above a solid horizontal line.

Gregorio Galicot (as agent for the carrier)  
President  
Faircall Corporation

Attachments: Accompanying Statement explaining CPNI procedures

## **FAIRCALL CORPORATION** **STATEMENT OF CPNI PROCEDURES**

Faircall Corporation ("Faircall") takes the protection of CPNI seriously. Faircall has received legal counsel in this area and protects the confidentiality of its customers' information. Faircall receives limited information from its customers and uses that information solely to perform the telecommunications services, for billing purposes and in response to legal process. It does not use this information for marketing purposes.

Faircall provides domestic telecommunications services, including public telephony, calling card, long distance operator assistance, credit card processing, billing, collection and wireless telecommunications services. Faircall processes casual-use voice services from telephone users making long distance calls from payphones and hotels. This process includes the collection of billing information and desired call destination from end users which eventually result in the creation of call detail records and include the date, time, duration, number dialed and billing number (the "Information"). The Information is collected from telephone equipment operators, and local and long distance carriers and is used by Faircall for calculating commissions and reporting this information via a secured website to sales representatives and customers; otherwise the information is restricted to authorized personnel, technical staff and network administrators.

### **Duty to Protect CPNI**

We recognize that carriers have a duty to protect customer CPNI. To the extent we obtain CPNI, we may not disclose CPNI to unauthorized persons, nor may we use CPNI in certain ways without consent from our customers. Before we can provide customers with their own CPNI, we must authenticate the customer.

We recognize that there are a few cases in which we can disclose CPNI without first obtaining customer approval:

1. Administrative use: We may use CPNI to *initiate, render, bill and collect* for communications services.
2. Protection of carrier and third parties: We may use CPNI to protect the interests of our company, such as to prevent fraud or illegal use of our systems and network. Employees are notified of the steps to take, if any, in these sorts of situations.
3. As required by law: We may disclose CPNI if we are required to by law, such as through legal process (subpoenas) or in response to requests by law enforcement. Employees are notified of any steps they must take in these situations.

### **Our Own Use Of CPNI**

We do not use CPNI to market to customers. Except as described herein, the Information is not made available to third parties by telephone, online, or in retail stores. The Information may be disclosed only (i) in response to proper legal process and (ii) for billing purposes, consistent with the provisions of Section 222 of the Communications Act. Access to the Information is available solely through a secure online network that requires authentication.

An individual's name and credit card number are collected when calls are billed to a credit card, and Faircall processes the payment and charges to the caller's credit card.

### **Authenticating Customers Before Disclosing CPNI**

We understand that we are required to objectively determine that our customers are who they say they are before disclosing CPNI to them.

#### **Telephone**

We do not release *call detail information*, or information relating to the transmission of specific telephone calls over the telephone. Our customers can only access this information through a secure, authenticated network.

#### **In-Person Authentication**

We do not release CPNI through in-person visits. Our carrier customers can only access this information through a secure, authenticated network.

#### **Mail**

If the customer requests CPNI through regular mail, or if the customer cannot comply with the authentication method above, we send the requested information to the customer's address of record only.

#### **Online Access**

We use strong cryptography and encryption techniques. For all web sites set up by Faircall, 28 bit SSL encryption is enforced for all pages where customer information data is present. For all communications with external entities sending customer information data to Faircall, strong encryption channels are set up, such as SSH, SSL, or SFTP. All Faircall administrative access to the web site machines uses SSH.

Faircall does not permit wireless networks to transmit customer information data unless an SSL channel has first been established.

### **Training And Discipline**

We have trained applicable employees regarding the company's CPNI policies. Employees will have an annual retraining to ensure that they understand the company's CPNI policies and any updates to those policies. New employees who will have access to CPNI are trained when they join the company, and then attend the regularly-scheduled retraining sessions. Employees are subject to disciplinary action for failure to abide by our requirements.

### **Record-Keeping**

We maintain records of discovered CPNI breaches, notifications to law enforcement regarding breaches, and any responses from law enforcement regarding those breaches, in our files for at least two (2) years.

### Unauthorized Disclosure Of CPNI

We understand that we must report CPNI breaches to law enforcement no later than seven (7) business days after determining the breach has occurred, by sending electronic notification through the link at <http://www.fcc.gov/eb/CPNI/> to the central reporting facility, which will then notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI).

We understand that we may not notify customers or the public of the breach earlier than seven (7) days after we have notified law enforcement through the central reporting facility. If we wish to notify customers or the public immediately, where we feel that there is "an extraordinarily urgent need to notify" to avoid "immediate and irreparable harm," we inform law enforcement of our desire to notify and comply with law enforcement's directions.

Records relating to such notifications are kept in accordance with our record-keeping policies. These records include: (i) the date we discovered the breach, (ii) the date we notified law enforcement, (iii) a detailed description of the CPNI breached, and (iv) the circumstances of the breach.

During the course of the year, we compile information regarding pretexter attempts to gain improper access to CPNI, including any breaches or attempted breaches. We include this information in our annual CPNI compliance certification filed with the FCC.

### Additional Protections

Faircall has established business procedures and policies to ensure protection of the Information. Faircall adheres to the Payment Card Industry Data Security Standard for protecting cardholder data.

Signed



Name

\_\_\_ Gregorio Galicot \_\_\_

Title

\_\_\_ President \_\_\_

Date

\_\_\_ February 24, 2010 \_\_\_